10th International Command and Control Research and Technology Symposium
The Future of C2

Implementing Network-Centric Command And Control

C2 Policy Track

Raymond J. Curts, PhD*
CommIT Enterprises, Inc.
5821 Hannora Lane
Fairfax Station, VA 22039-1428
(C) 703-731-0301
(F) 775-254-4248
rcurts@ispwest.com
Primary Point of Contact (POC)

Joseph P. Frizzell, PhD
ASD(NII) C2 Policy Directorate
Crystal Mall 3, Suite 6000
1851 South Bell Street
Arlington, VA 22202
(C) 703-607-0713
(F) 703-607-0658
joseph.frizzell@osd.mil

* Primary Point of Contact (POC)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Implementing Network-Centric Command and Control	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **CommIT Enterprises Inc,5821 Hannora Lane,Fairfax Station,VA,22039-1428**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**56**	

Implementing Network-Centric Command And Control

Raymond J. Curts, PhD*
CommIT Enterprises, Inc.
Fairfax Station, VA
(C) 703-731-0301
rcurts@ispwest.com

Joseph P. Frizzell, PhD
ASD(NII) C2 Policy Directorate
Arlington, VA
(O) 703-607-0713
joseph.frizzell@osd.mil

ABSTRACT

This paper examines implementation issues associated with integrated, network centric Command and Control concepts, and highlights significant challenges inherent in such a transformation from the current C2 environment within the U.S. Department of Defense (DoD). The authors argue that it will be some time before military forces can achieve a truly integrated command and control capability because significant impediments relating to the ***culture, structures, processes, and products*** *remain to be addressed.*

We begin by examining current developments in net-centric, service oriented and effects based operations as part of the changing nature of the U.S. military operational environment. Recent developments in command and control policy, processes and governance are highlighted, and the inherent social challenges related to achieving interoperability are briefly discussed. We examine the framework of Integrated Command & Control (IC2) and argue that development of such a capability must be based upon a shared purpose realizing that it will require a significant amount of time and patience. We then propose the way ahead by addressing the ingredients needed to achieve an IC2 capability within the U.S. Department of Defense. These include: working on the cultural and human engineering aspects of C2; creating a different, more diverse learning climate; tackling the issues of jointness, demonstrations and experimentation; and addressing the need to have an immediate, constant flow of visible deliverables to sustain the transformation journey[†].

---

* Primary Point of Contact (POC)

† This paper is based upon and is a continuation of research originally begun by LTC Seng Hock Lim of the Singapore Armed Forces while enrolled at the Canadian Forces College [Lim, 2003]. It has been adapted here to the United States Department of Defense and the U.S. Armed Forces.

Introduction

> *"By making possible a faster, clearer reading of the situation and a more effective distribution of resources, a superior command system may serve as a force multiplier and compensate for weaknesses in other fields…"* [1]
>
> - Martin van Creveld, 1985

In the near future, can a commander really command and control his forces and synchronize actions to disrupt adversaries over vast distances by a mere click of a computer mouse button? Would an enterprise-wide, Integrated Command and Control (IC2) system present an Achilles' heel to a potential adversary rather than enabling optimum resource utilization and responsive combat power? What about the issue of interoperability in the new security environment presented by net-centricity and the Global Information Grid (GiG) where multi-agency, allied and coalition operations will become common? What are the implications to the Armed Forces during its transformation journey? This paper will attempt to explore these questions and examine recent developments in these and related areas.

The field of Command, Control, Communications and Computers (C4) is moving so quickly that the interaction between user pull and technology push is becoming exceptionally dynamic. Advancements in C4, sensors, information, information systems and precision-strike technologies, as well as the implementation of new, broad, ubiquitous networks, are creating a significant change in the military information environment.

New ways of thinking about Command and Control (C2) are at the heart of Information Age Warfare [Alberts, 2001]. The increasing complexity of military weapons systems, military organizations and war-fighting itself, has created an ever-increasing demand for and reliance upon information technology systems [Manfred, 2002]. The emergence of what has been termed the Revolution in Military Affairs (RMA) is generally accepted by many military services as the future of C2, i.e. the advent of knowledge or information age warfare. Information age technologies could potentially be the key to dissipate old dictums about the fog and friction of war by fundamentally changing a military commander's ability to "see", to "tell", and to "act" [Owens, 2000] or, as portrayed by Col. John R. Boyd, USAF, to "Observe, Orient, Decide and Act (OODA)" [Boyd, 1986].

Information technology advancements are enabling modern armed forces to undergo a fundamental shift from a platform-centric orientation to a net-centric, service-oriented one. Recently, the concept of Network-Centric Warfare (NCW) has been widely discussed. Net-Centric operations are military operations that are enabled by the networking of the force [Cebrowski, 1998]. As such, perspectives about the process of command and control can change fundamentally. A robustly networked force will be integrated vertically by the network, through all command echelons – from strategic down to the lowest tactical level [Potts, 2002a]. While it is usual to focus on the

technology portion of the information age influencing the evolution of command, the effect should be viewed as more than just a better, more effective C2 system.

This paper examines the concept of network centric operations and integrated command and control in the information age. It highlights some of the significant challenges faced in embarking on this type of a transformation journey. The premise is that it will be some time before U.S. military forces can achieve a truly integrated command and control capability because significant impediments relating to the **culture, structures, processes, and products** must first be addressed.

The RMA Debate

The notion of military revolution grew from Soviet writings of the 1970s and 1980s analyzing the revolutionary potential of new military technologies [Cooper, 1994]. As Marxists, the Soviets were comfortable with the idea that history is driven by revolutions. Western analysts, however, were more focused on technology. Today, the technical impetus to an RMA remains foremost in most related studies. By one definition, RMA is "… a major change in the nature of warfare brought about by the innovative application of technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts fundamentally alters the character and conduct of military operations" [Watanabe, 1995]. A common goal is the synergy that advances in communication and computers can bring to the information application and management arena.

An estimate of approximately 18 months for the doubling of computing capacity and processing power, a common interpretation of Moore's Law[2], still appears to be roughly applicable today. This implies a continued and powerful growth in the ability to process a great amount of information with increasing responsiveness. The cost of computing has also fallen dramatically. Until recently, networking was far too costly to realize the value proposition embodied in Metcafe's Law[3] [Alberts, 2003a]. While bandwidth has become cheaper and more widely available,[4] for the "communication hungry" military, there is often still a significant bandwidth deficit [Peter, 1998]. This is true especially in the context of wireless C2 information systems if large files or bandwidth intensive applications, such as map overlays and video conferencing, are demanded indiscriminately.

Many analysts of the RMA have argued that technological breakthroughs will have a major effect on how operations will be conducted in the future. The Gulf War is often cited as an example of how these new technological advances can be employed on the battlefield, based upon the success of the high tech weaponry and the command and control systems of U.S. forces [O'Hanlon, 2000]. Some also argued that the rapid conduct of Operation Allied Force[5] and the wide-spread use of precision-guided munitions provides further evidence that we are on the verge of a change in how war will be conducted in future [Young, 2003].

Although generally accepted, the RMA debate continues because there are several different views of an RMA. O'Hanlon, for example, identifies four main RMA schools. These range from a cautious approach acknowledging the contemporary RMA hypothesis (i.e. system of systems approach), to a bold assessment of global revolution involving the whole spectrum of technology [O'Hanlon, 2000]. Revolutions imply periods of rapid and fundamental changes and are hard to predict because of the expected disruptive effects. There can be little doubt that further scientific revolutions will occur and any defense planning that looks more than 15 to 20 years ahead must be flexible enough to take account of the potential offered by the radically new technologies that might emerge [May, 2001]. However, if indeed there is an information led RMA, technology alone cannot decide the outcome. It is necessary to combine hardware, quality training, sound doctrine and effective organizations as an integrated whole.

For U.S. forces, new challenges are constantly emerging (e.g., the rise of trans-national terrorist threats such as the Al Qaeda network). The U.S. military must be prepared to face future challenges while meeting the demands of the present. As such, there is a need to have greater flexibility and robustness in the developmental approaches. In a recently published monograph, the need to begin the transformation journey and to meet the complex challenges of technological discontinuities, asymmetry and globalization were emphasized [JSAF PM1, 2003]. The ***capacity to change*** is as much about assessing fundamentally different strategic options as it is changing the ***mindsets*** of people to dare to look at radical changes and to experiment. The ***military culture*** is an important consideration if revolutionary operational concepts are to be tested successfully.

NCW And Effects Based Operations Development

It would be tempting to think that the exploitation of information age technologies in the military environment is essentially a communications, information system or staffing process issue or that this will result in a substantive outcome, which will be a more effective command and control system, and that it can be left primarily to those responsible for developing our command and control systems [Potts, 2002a]. However, if a more effective C2 system is intended to fight in a very different way, it must be understood and applied by commanders and warfighters, not just technical staff.

Over time, information age technology can be exploited by emphasizing an integrated battlespace through the advantage of networked capabilities. The shift will be towards a net-centric environment with integration throughout a theatre of operations and between theatres of operations. The emphasis will be on exploiting networked capabilities to apply integrated joint effects to precise effect. "There will be greater emphasis on connectivity between sensors, weapon platforms and C2 nodes, and less emphasis on numbers of weapon platforms." [Potts, 2002a] These are the essence of what is commonly termed Net-Centric (or Network-Centric) Warfare (NCW).

In a way, NCW provides the theory of warfare in the Information Age. It is, as the NCW Report to the U.S. Congress stated, "no less than the embodiment of an

Information Age transformation of the DoD."[6] [Alberts, 2003a]. It was stated that net-centric warfare and all of its associated revolutions in military affairs "… grow out of and draw their power from the fundamental changes in American society …." [Cebrowski, 1998]. Basically, the argument was that the underlying economics (IT is central to competition based on return on investment) and the underlying technologies (e.g., explosive growth of the internet and use of network-centric computing) had changed. Along with the changes in the way business is conducted,[7] the military must also adapt.

NCW is characterized by information sharing, shared situational awareness and the knowledge of commander's intent. As described in the Network Centric Warfare Report to Congress, a fighting force that can conduct network centric operations can be described as having the following attributes and capabilities [DoD, 2001]:

- **Physical Domain**: All elements of the force are robustly networked achieving secure and seamless connectivity.
- **Information Domain**: The force has the capability to collect, share, access and protect information. The force can collaborate in the information domain.
- **Cognitive Domain**: The force has the capability to develop and share high quality situational awareness and have a shared knowledge of the commanders' intent.

All of these domains require a *shared* networking environment, *shared* information and knowledge, *shared* situational awareness and understanding of commander's intent. By definition, *shared* implies [Encarta PD]:

- The use of something along with others.
- Letting someone use something.
- Having similar feeling or experience.
- Taking responsibility together.

So, besides the physical, information and cognitive, domains the **social domain** (the domain of sharing) is also needed. Interoperability in the social domain ultimately allows actions to be dynamically self-synchronized (the ability of commanders to support one another without detailed prior coordination due to shared awareness).

- **Social Domain**: The social domain implies the **cultural** impact that can create the kind of understanding that will promote *shared* interaction and proceedings congruent to the commander's intent.

C2 processes and the interactions between and among individuals and entities that fundamentally define organization and doctrine exist in the social domain.

In Alberts' book Power To The Edge he states that the principles of "power to the edge" can be applied to both the organization and management of work, and the design and architecture of systems. Its applications to the organization and management of work is primarily about C2 in the cognitive and social domains. While its application to the

info-structure relates primarily to C2 in the physical and information domains [Alberts, 2003a].

One of the major insights that has emerged as a result of ongoing NCW initiatives is that the combat power associated with net-centric operations is non-intuitive [Garstka, 2003a]. Hence, the likelihood is that warfighters will develop new tactics, techniques and procedures only after they have had the opportunity to operate and train with an information advantage and develop trust in the network environment.

In spite of a ponderous acquisition process, technology insertion is ahead of and disconnected from joint and service doctrine and organizational development [Cebrowski, 1998]. This is perhaps one of the reasons why the impediments to progress have also been a subject of debate in the literature. In a recent article on learning lessons about NCW from Operation Iraqi Freedom, it was mentioned that a retired U.S. Marine Corps General had said that many personnel still "… have no clue what it is …." and that "… there's a significant communications problem at the tactical units who were out of contact except for satellites …." [Caterinicchia, 2003].

For NCW to be useful, it must be applied to military operations. This is important especially to the operational-level commanders who need to translate the concepts to application in the theatre of operations. Military operations, in the new security environment, will span across the spectrum of operations from peace, to crisis and to war. The common term that is increasingly used to describe the process to shape the desired result is Effects Based Operations or EBO.

EBO (military operations directed at shaping the behavior of foes, friends and neutrals, in peace, crisis and war) constitutes the conceptual framework for a two-step process of turning net-centric capability into a national advantage [Smith, 2002]. In a way, EBO is not entirely new thinking since using military forces to shape the behavior of opponents and allies has been practiced since Sun Tzu or longer. EBO can transcend the levels of operations in order for strategic, operational and tactical objectives to be attained. David Deptula, an early proponent of the concept of EBO [Deputla, 2001], provided a catalyst for much of the conceptual development and debate. Initially, the proponents were mainly from the U.S. Air Force due to the emphasis on air power to achieve strategic effects.

Adaptation to the Information Age will mean an understanding of what NCW and EBO can bring to military operations while bearing in mind that these are still largely terms used by U.S. researchers and they do not imply a replacement of earlier forms of warfare. However, they do present a possible synergistic approach to looking at military transformation. EBO encompasses the focus on the mission and the conditions of military operations, while NCW provides the framework and the tools. They both deal with the why, what, how and support of military operations [Deputla, 2001], which are crucial to looking at the military transformation journey.

Transformation In The Information Age

While some may argue that the NCW is not optimized for asymmetric warfare[8] and low intensity conflict, NCW is a key component inherent in the latest term used in the conceptualization of RMA - *transformation*. It was reported that the information networks established for the United Kingdom's Iraq War forces paved the way for the country's force transformation [Ackerman, 2003]. Some of these efforts were driven by the need to interoperate with vital U.S. C4I systems that were rife with imagery.

Worldwide, many modern military forces have crafted their own individual responses to the challenges and opportunities of the information age. NCW is a common term used by the armed forces of the United States, Denmark, Norway and the Netherlands. Other terms coined include Australia's network-enabled warfare,[9] the United Kingdom's network-enabled capability, the Swedish Armed Forces' network-based defense and the Singapore Armed Forces' knowledge-based command and control [Garstka, 2003a].

What does the term transformation mean? Dr. David Alberts described transformation as "… a process of renewal, an adaptation to environment …." [Alberts, 2002]. Essentially, transformation means adapting to significant changes while failure to do so would imply significant risks. Alberts argued that potential adversaries can also take advantage of the low cost of obtaining "Information Age technologies" and inaction is not an option in a transformation strategy. Pushed by the U.S. Secretary of Defense, Donald Rumsfeld himself, the need to transform is seen as important due to the changing environment (spectrum of operations) and different, emergent threats, as the capabilities are continually evolving.

However, while there are indeed remarkable improvements in developing *warfighting* concepts in the U.S. Armed Forces, the same progression has not succeeded in creating truly ready joint forces in *peacetime* and the related rationalization of capabilities in the services [Snider, 2003]. This may be offset by recent developments in the Pentagon where the Joint Staff will exercise greater control to ensure that efforts by the services are not duplicated [Sherman, 2003]. Five Functional Capabilities Boards (FCBs - force application, force protection, battlespace awareness, focused logistics, and command and control) have been created to spearhead the analysis, prioritize needs, and advise acquisition authorities.

In the context of U.S. forces, the IT landscape has changed significantly and the quest to achieve a high level of competencies in IT related skills among the troops is clearly producing results. Today, U.S. forces have developed into a military that is technologically focused and professionally respected. However, this has also impeded the impetus to change radically for fear of upsetting efficient and well-established procedures. As such, the transformational journey must focus on the ***people*** aspects and involve the operational commanders and their forces by enabling them to be part of the capability concepts development. For example, they can help to review and validate

some of these concepts during exercises and demonstrations. One of the key desired outcomes, to be discussed shortly, would be the ability to implement an integrated, enterprise-wide C2 system that can significantly increase the desired combat effects for a spectrum of operations. Separating command and control (C2) from the third C, Communications, the enabler of C2, makes re-conceptualizing command and control all that much more mystifying.

Re-Conceptualizing Command And Control

Command and Control: The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission [JP1-02, 2003]. The establishment of common intent to achieve coordinated action. C2, in its historical context, refers to the structures (real and imagined), processes, technologies, and people that comprise the system. For a commander to have effective C2, the system must enable him to make timely decisions and take appropriate action.

Command: 1. order, 2. control, 3. thorough knowledge, 4. operating instruction to computer, 5. authority, 6. military control, 7. something under officer's jurisdiction, 8. group of officers in control, 9. military group with specific function. [Encarta PD]

Command: 1. The authority that a commander in the Armed Forces lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel. 2. An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action. 3. A unit or units, an organization, or an area under the command of one individual [JP1-02, 2003].

Control: 1. restrain or limit, 2. manage, 3. oversee affairs, 4. ability to run something 5. limits and restrictions, 6. supervising person or group. [Encarta PD]

The terms ‘command’, ‘control’, and ‘C2’ are often used in military literature. They are supposed to be quite entrenched in the doctrinal and operational “dictionary.” However, their usage can be said to be “abused” and it is probably true to say that a number in the military may sometimes be confused by the context of their usage. In fact, at the time of this writing, multiple “new” definitions have recently been proposed. After some research, Pigeau and McCann remarked “… there was little consensus within either the military or the research communities on the actual definitions for Command, Control and C2 ….” [Pigeau, 2002].

Historically, the topic of command has been extensively discussed and much has been written regarding its methodologies and practices. The term command and control

(C2) appears to be more recent. Command as defined by the U.S. military (and quoted above) includes "… responsibility for effectively using available resources, planning the employment of, organizing, directing, coordinating and controlling military forces for the accomplishment of assigned missions. It also includes the responsibility for health, welfare, morale, and discipline of assigned personnel."[10] As such, control is subsumed as a part of command. Control is more than a feedback mechanism since **structures and processes** must be put in place to facilitate accomplishment of the mission [Pigeau, 2002].

It may not be fruitful to force a distinction between command and control. Two common distinctions include art (command) and science (control), and the commander (command) and his staff (control) [Pigeau, 2002]. The U.S. Dictionary of Military Terms definition of C2 refers to the facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned [JP1-02, 2003]. The U.S. Army has also published a new C2 doctrine (Field Manual 6-0, *Mission Control: Command and Control of Army Forces* [FM 6-0, 2003]) to take into account the development and use of modern IT and "… their powerful ability to influence the conduct of operations …." [Connor, 2002].

The authors believe that it is better to refer to C2 in the context of processes to achieve the accomplishment of the mission, from formulating courses of action to monitoring execution and giving orders. However, a growing number of those who are looking at command and control in the Information Age have concluded that the terms need to be clarified and brought into the 21st century [Alberts, 2003a], without being constrained too tightly by historical references, nor encumbered by the communications systems that make them a function.

Pigeau and McCann took a new look and defined the two terms separately and in an interesting way: [Pigeau, 2002]

> "*Command*: the creative expression of human will necessary to accomplish the mission."
>
> "*Control*: those structures and processes devised by command to enable it and to manage risk."

They place an important emphasis on the human aspect of command that can achieve outcomes through motivation, means and opportunity. They include a model to distinguish command that incorporates three factors: Competency, Authority and Responsibility. Their definition of C2 is the establishment of common intent to achieve coordinated action[11]. Hence C2 structures must have the ability to stay *flexible* to meet evolving needs even as continual learning and change should be encouraged and rewarded.

C2, in its historical context, refers to the structures (real and imagined), process, technology, and people that comprise the system [Sharpe, 2002]. For a commander to have effective C2, the system must enable him to make timely decisions and take appropriate action. The well known Observe, Orientate, Decide, Act cycle (OODA Loop)[12] allows new thinking in reducing the decision-action cycle. It has an intuitive appeal, resulting in the common phrase used by many commanders: "… operating inside the enemy's OODA loop …."

The OODA loop, when applied in the information age context, may appear too simple. For example, it was noted that OODA cannot model correctly the differing C2 processes, both in terms of function and timescale, which are carried out at various levels of command [Thackray, 2002]. One of the more useful models to study when considering the network-centric portion of C2 processes is provided in Figure 1 below.

The illustration consists of three domains that define military activity, which were described earlier as the attributes of NCW. Here, the physical domain consists of the operating environment (entities outside the C4ISR[13] processes and systems) while the cognitive domain refers to the minds of the participants. Within these domains, the interacting elements include battlespace monitoring, awareness, understanding, sensemaking (how situations may develop), command intent, battlespace management (command intent translated into activity) and synchronization [Thackry, 2002].

This illustration allows one to look at the cognitive domain with the aim of ensuring a better understanding of the situation and commander's intent. Battlespace monitoring and management are included in the NCW aspects (i.e. sensors' system of systems and seamless information grid). A **shared understanding** of the operational situation at all levels of command should provide the stage for mission command to flourish and enable an unprecedented tempo of operations and effectiveness of maneuver and engagement [Thackray, 2002].

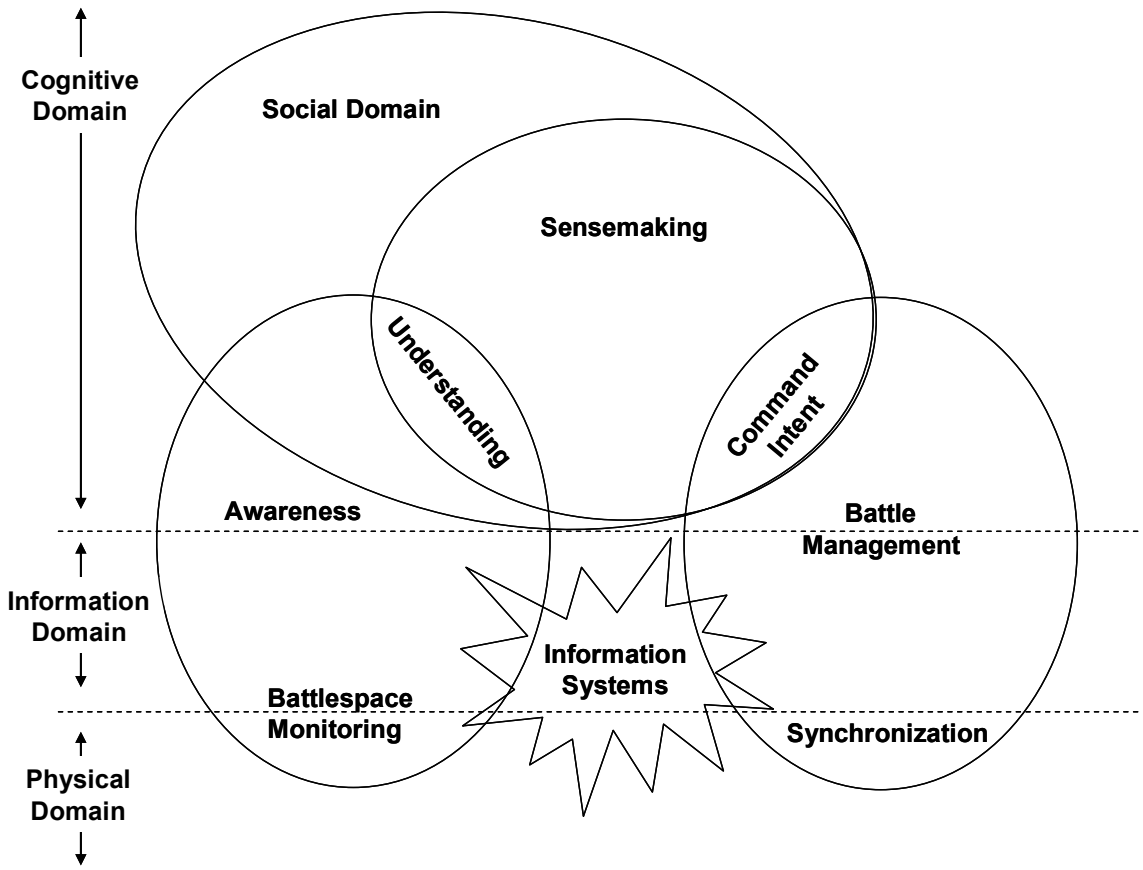


Figure 1: The Information Age C2 Process[14]

This, Alberts proposes, can enable greater integration with a networked C4ISR and the information systems embedded in it [Alberts, 2001]. Integration also implies it will have great impact on the interoperability issue as well. The authors' concept of where the **Social Domain** might lie is shown as an overlay to Alberts' original diagram in Figure 1 above.

Interoperability

To have an effective and robustly networked force, there is a need to have an enterprise-wide, integrated C2 system. Such a force can only be achieved if there is high interoperability among mission participants, data elements and the systems that support them. Interoperability ensures the ability of systems and forces to interact effectively with other systems and forces. Forces that are interoperable are able to operate in a net-centric environment. Besides the domains of *physical, information* and *cognitive*, the ***social*** domain is also needed. Interoperability in the social domain allows actions to be dynamically self-synchronized (the ability for commanders to support one another without detailed prior coordination due to shared awareness, in other words*, **trust)***

[Alberts, 2003a]. Again, the social domain implies the **cultural** impact that can create the kind of understanding that will promote interaction and actions congruent to the commander's intent.

The events of 11 September 2001 and the resulting coalition efforts amplified the need to address interoperability among forces from different nations, departments and agencies. Technology has made it easier in the quest for interoperability but there are still many challenges to overcome. While global communication systems can enhance connectivity and emerging technology can create superb surveillance systems, the integration of coalition forces may not be easy.

Attaining technological interoperability will be difficult for coalitions in any case [Scales, 1998]. The Gulf War saw participants arrive with different levels of technical sophistication and hence there were incompatibilities among systems. Also, the tremendous rate of change in IT implies that obsolescence will be a constant worry for those attempting to maintain interoperability. To a theatre commander in coalition operations, the technological gap (e.g., with less IT savvy participants) can be partly overcome by extending training means and methods. This will entail extra manpower and effort.

For the many nations, technology is not the only obstacle to coalition operations. In a recent presentation, a coalition General officer stated that the goals, culture, doctrine, logistics, status of coalition partners and the sense of ***trust*** are all important factors to consider.[15] For integrated C2 to be achieved in coalition operations, the command structure and relationships between commanders are important considerations. Command and control can be based on certain models from past operations, but it does require the appointment of a capable and credible coalition commander acceptable to all. In most regions where the diversity of interest and motivation is significant, the use of operational control under the United Nations (UN) model is regarded as appropriate [Ayling, 2001].

The future operating environment is likely to see more coalition type operations. Even in limited wars, C2 technologies cannot be ignored as they can provide commanders with unprecedented levels of situational awareness and other significant warfighting advantages. The U.S. has taken a leading role in the interoperability issue. One example of these efforts related to C2 is the Joint Warfighter Interoperability Demonstration (JWID) which aims to provide commanders in a combined task force with improved C4ISR capabilities to meet the interoperability goal.

Many regional exercises are conducted to strengthen this aspect of development. For example, Exercise Cobra Gold in 2002 (participants from Thailand, Singapore and U.S.) saw eighteen other countries sending observers, a 100-percent increase since 2001 [Fargo, 2003]. Still, the U.S. is likely to need "legacy" system compatibility to operate with coalition partners since not many of the nations could keep pace (for financial reasons among others) with the more advanced technologies used. This issue is

compounded if **proprietary systems** are being fielded as well as when **security considerations** hamper systems sharing data seamlessly.

Integrated C2 (IC2)

The central idea of IC2 is the superior collection and organization of knowledge to provide dominant situational awareness at all levels of command thus achieving more effective command and control of forces and the precise application of effects [Mahmud, 2003a]. IC2 aims to maximize combat effectiveness and gives the services a quantum jump in capabilities within the constraints of its resources. Command and control is as much about the technology and the **processes** that enable it, as it is about the commanders and their staffs who use the technology and processes. *Integrated* refers to the need to fight as an synchronized, harmonized, multi-dimensional force. The U.S. military is still largely organized along Service lines (especially within the acquisition arena) and, since we perceive a need to plan on the basis of the entire spectrum of military capabilities, one of the most basic requirements is the integration of the command and control system.[16]

IC2 enables the military to engage in NCW through the use of advanced C4 and IT technology. In a network environment, an integrated approach that allows sharing of data, information and knowledge can be embedded in decision support systems, allowing commanders and their staffs to focus on core issues rather than technical analyses. IC2 works as an enabler throughout the OODA loop across all four domains mentioned earlier. Represented in Figure 2, IC2 aims to "see first, see more" and therefore will result in better understanding and decisive action. It is envision that IC2 will enable fully integrated, knowledge-based warfighting concepts to be operationalized and contribute to a more flexible and flatter C2 structure. If the speed of decision-making also increases, then this will enable a higher tempo of operations to be effected.

What does IC2 imply to the commanders and men? While there is little doubt that IC2 can change the way we think and the way we fight, much more must be done with the main components of force transformation: ***culture, process and product***. While IC2 builds on the force's comparative advantage of having a relatively large number of techno-savvy people, the development and subsequent changes must be based on a shared purpose approach from the commanders down to the lowest level. After all, integration in C2 implies working towards a common purpose by maximizing available resources.

While the "fruits" of IC2 will not be so quick to emerge due to the existing gap, dialogue at all levels of command should always be maintained to highlight development issues and measure progress, e.g., testing of concepts and results of C2 related experiments. Intermediate products and knowledge gained (whether successful or not) should be shared widely. All of these efforts will require patience and time. To achieve the next big leap in capability, IC2 *cannot be the dream of just a few and remain distant and vague to the rest.* Transformation is indeed about moving forward and its relevance to the soldier should be continuously revisited so that the journey is made as a cohesive

force. Intermediate products and results are an essential part of getting and keeping the process going.

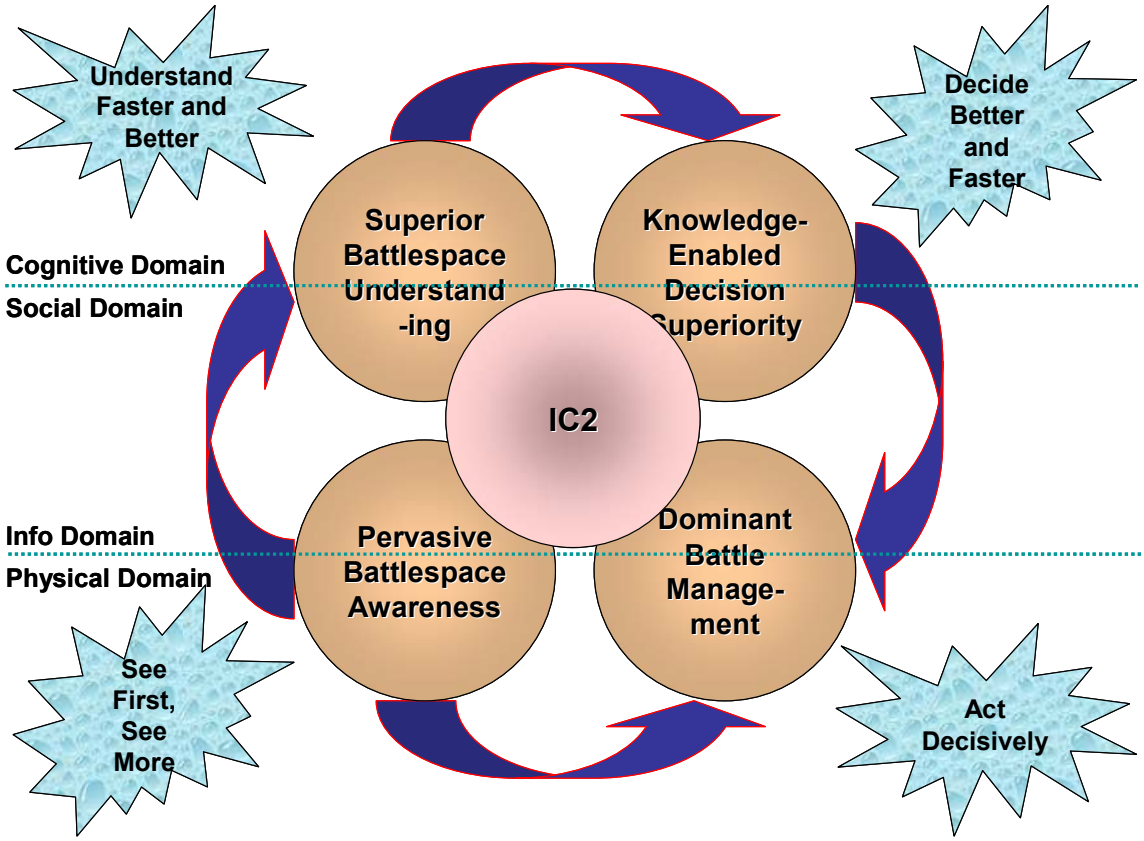


Figure 2: Integrated Command and Control Framework[17]

The Way Ahead

It is not an easy task to embark on the transformation journey and ensure the success of IC2. Indeed, short-term pain versus long-term gain is a recognized issue since, initially, adherence to standards and requirements under the IC2 framework will possibly slow down the current pace with which individual systems and capabilities are fielded [JSAF PM1, 2003]. What then are the main considerations and ingredients needed to create and achieve NCW and IC2 Capabilities?

Key Ingredients: Technology alone cannot dictate the outcome of war. It is necessary to combine hardware / software systems, quality training, sound doctrine and effective organization to produce a lethal fighting force. The following are considered key to achieving IC2:

Culture

The *capacity to change* is as much about looking at fundamentally different strategic "options" as it is changing the *mindsets of people* to "dare" to look at radical changes

and to experiment. The **military culture** is an important consideration if revolutionary operational concepts are to be tested objectively and evaluated fairly.

According to retired Navy Vice Admiral Arthur Cebrowski, not enough of the technology that drives NCW is finding its way into the hands of the warfighters. In addition, a ***change of culture*** is needed to prepare the warfighter to adopt the technology [Cebrowski, 1998].

The issue of ***culture*** is an important consideration and is a key factor to consider if U.S. forces are to succeed in the transformation journey. It has been argued that Western armies have progressed significantly over the years because of "… a long-standing Western cultural stance towards rationalism, free inquiry and the dissemination of knowledge …." [Hanson, 2001]. An overall cultural landscape that encourages and supports these qualities can, therefore, afford inherent military advantages in terms of the way thinking and innovative ideas are developed.

In order to induce understanding and develop commitment, it must be clear to the commanders and warfighters what we are changing and why. Inherent in this, is a need for a credible communications plan. The services have shown tremendous capacity to adapt and are very good in a task-oriented type of environment. Rigorous debate, discovery and experimentation among warfighters, defense academics and defense scientists necessitate a very different learning climate. Efforts towards grasping the fundamentals of organizational learning at various command levels and training schools will support this effort. The Services have already embarked on similar initiatives. Consequently, we must ensure that our policies support and encourage a spirit of learning and sharing that transcends the services, major commands and other organizational units. The challenge is how to make this become an integrated effort since IC2 is based on the concepts of shared understanding and shared awareness.

People

As mentioned earlier, along with culture, one of the key ingredients in achieving IC2 is ***people***. After all, culture, by definition, is "… people with shared beliefs and practices …." [Encarta PD] The importance of people is often cited in reports of change and to really enable transformation and harness the power of IC2, the need for a common purpose cannot be ignored if we intend to accelerate the change. The development process, as argued previously, and well accepted by planners, will take a long time. Few, if any, can afford the kinds of resources and the capital expenditures devoted to the transformation that DoD has incurred thus far. The services, with limited resources, must work out an overarching set of policies supporting core capabilities that forces can understand and implement.

Trust

Trust is a major component of the social domain. ***Trust*** is believing. It alleviates having to confirm or verify, and eliminates the requirement to know first hand that something has been successfully accomplished. Trust is an learned quality derived from faith in the system and those who are part of it, and is based on mutual understanding, commitment, conviction and dedication. This becomes a part of the culture, and, as we have shown, culture is an integral element of the social domain.

Time

The ***time*** factor highlights further the need to share this journey. The excitement surrounding a technologically enabled transformation could quickly fade if progress is not timely. The operations tempo can not be allowed to increase unchecked to support a wider spectrum of operations. Hence, policy must clearly define roles and responsibilities, and commanders must set priorities such that work objectives are defined at manageable levels to fit within existing time constraints. With clear cut policy and the commitment of the leadership, service members at all levels of responsibility can feel that they are part of this transformation process, rather than casual observers subjected to it.

Structures

Another ingredient involves the difficult aspects of ***structures*** and processes. To be able to fight in an integrated manner and across a wide spectrum of operations, the issue of "jointness" should be carefully addressed. The need to be modularized and task force oriented for better responsiveness and agility are already quite well accepted. However, what this entails in terms of being able to fight in an integrated manner, and enabling commanders to have superior C2 in operations may not be that simple. Sun Tzu observed that "… just as water retains no constant shape, so in warfare there are no constant conditions …," emphasizing the need to have continuous adaptation and superior battlespace awareness and understanding [Tzu, 1985]. This fluidity, however, strains C2 resources and significantly increases the complexity of policy development.

The faster and more complicated war becomes, the greater the need for close, continuous cooperation among the Services [Seet, 2003]. With a tight defense budget, synergy must be obtained by channeling the competitive environment among the Services towards a productive purpose. Hence the sense of purpose remains important. Flexibility and versatility must be sustained in order to achieve operational success. At the highest levels, policy must provide structure without limiting this flexibility. Decision-making can be decentralized if commanders' intent is clearly conveyed and understood. IC2's network structures contrast with the hierarchical nature of the current military structure and a major revamp may be needed.

Processes

Well defined and tested ***processes*** are necessary to support the structure and the full spectrum of joint operations envisioned by the Goldwater Nichols legislation. Joint forces, able to "plug" quickly into an integrated battlespace structured around interoperable communications, standards, doctrine, tactics and procedures, benefit from greater adaptability and a superior sense of battlespace awareness. Joint operations are best suited to benefit from the information revolution through seamless information and knowledge interaction, which continues to be constrained, though to a lesser degree than in the past, by Service parochial interests. OSD is committed to the transformation of C2 by encouraging new joint operational concepts and joint experimentation. Such exploration requires the active participation of commanders and warfighters so that they can feel the tempo change and can contribute immeasurably to process development. A responsive technology transition mechanism and a streamlined acquisition process are critical to the success of the entire effort.

Activities that are important to adopting process changes include clarifying the new operating concept, developing new training methodologies and adopting an experimental approach. The establishment of some sort of Future Systems Directorate could be a commitment towards transformation by focusing on exploring new operational concepts and experimentation. However, such exploration would still require the active participation of commanders and men so that they can experience the change in temp and develop a certain sense of ownership. It should not be taken as a validation exercise by troops and the emphasis must be that it is "*safe to fail*", a significant change in the mindset of military personnel. Experiments and lessons learned from operations or exercises can be the source of emerging doctrine, or else there will be significant lags in doctrine and policy development.

In fact, in order to have the creativity necessary to embrace NCW, IC2 and effects-based planning, a "*dare to experiment*" attitude would enhance the process of adapting and learning. Likewise, while training, evaluation and validating doctrines are necessary activities, a fresh look at the training process would be fruitful. This should include new learning methodologies (e.g., knowledge-based approach, experiential and team learning, adaptive thinking) and new doctrines (e.g., integrated, joint, multi-national coalition operations). With such an approach, some of the major obstacles related to C2 development like information overload (especially in headquarters facilities) and bandwidth constrains, can have more emphasis. The danger of relying on higher echelons having the best situational awareness could result in high-level commanders trying to be involved in minor tactical maneuver and operations. Situational awareness must also filter to the lower levels of command.

Products / Deliverables

Yet another ingredient is related to ***products***. Here, **visible deliverables** become important, both politically and operationally, to sustain the transformation journey towards IC2. Products that are based on an integrated C2 architecture will give the

services a quantum leap in capabilities when combined with battlespace awareness and precision strike. Products for the tactical levels cannot be ignored and while operating in wireless mode still present significant technical challenges for mobile forces (e.g., bandwidth and reliability), intermediate products have to be tested so as to enhance the learning curve. Service commanders need to grasp the implications of being able to operate in an integrated manner with new technologies that enhance the understanding of C2 requirements in the information age.

Products, while needing to leverage technology, can also be in the form of learning from the experimentation process. This would help develop the key competencies required to be familiar with operating in a network environment. An overarching, enterprise-wide architecture needs to be developed and communicated quickly so that integration can at least begin to take shape, even though changes and fine-tuning to the architecture will be expected. However, experimentation and products inevitably imply the commitment to capital investments. Also, the more we rely on information resources and systems, the greater must be our efforts to protect them [Chia, 2003].

Organization

Within DoD there are currently multiple ***organizations*** with varying levels of responsibility for C2 functions, processes, procedures, policies and operational concepts. In addition, each of these organizations sponsors a number of C2 or C2-related initiatives and there does not seem to be any central coordination that will ultimately ensure an enterprise-wide IC2 environment. Even if these were all perfectly coordinated, the construct is extremely difficult to work within. Some organizations / initiatives are focused on tactical / theater C2, some are nationally / globally / strategically focused, and still others are related to missile C2, maritime C2 or a whole host of other, mostly artificial classifications. At a very high level with DoD, it is essential that some overarching coordination activity take place.

Fragmented organizational responsibilities lead to fuzzy boundaries and questions over the roles of the organizations involved. Clearly, a well thought-out, workable organization, possibly a single common C2 governance structure, is required. Some agency must accept the responsibility for and be empowered with the authority to:

- integrate / coordinate C2 architectures and programs across DoD,
- assist with the development of and endorse C2 policies and directives,
- represent the C2 community at large within the Integrated C2 enterprise-wide governance structure.

Ultimately, investing in IC2 as part of force transformation will have an impact on resources and on efforts tied to force readiness and near-term force development. The children of today are acquainted with computer games and, as a result, are good at operating in a virtual environment (e.g., “button-pressing” to shoot at “enemies” while playing a combat game). However, military operations have become more complex and transformation will require more than just a few quick twists of a computer dial. Indeed, arguments have been raised regarding the possible vulnerabilities of IC2 (e.g., easier to

attack and exploit an integrated network, new innovations by adversaries, inherent chaotic nature of operations, etc.). There are also implications to servicemen relying too heavily on technology since machines as yet cannot match the judgment capability of human minds. The "champions" of the IC2 journey need to be aware of such possible pitfalls.

There must be governance to support and enforce the development a *culture* of *trust* within and among *people* and *organizations*, to adhere to *time*-frames and to develop the *structures*, *processes* and *products*, that will deliver the full range of Integrated C2. And lastly, all of the above must be coordinated. DoD is a very large organization with significant functional overlaps among offices, and insufficient coordination of efforts which result in duplication of expenditures, capabilities and other inefficiencies. Policy, guidance and governance are the sort of glue that will help to coordinate and hold the key components together.

Conclusion

In the past decade alone, we have seen tremendous development in the use of information technology for military peacetime information systems and wartime command and control systems. The security environment today has a hazier distinction between war and peace since peacekeeping, homeland security and the war against terrorists have shown that the military must adapt to a wide spectrum of operations and venues. While the development and acquisition of hardware will continue, the opportunity is there to move ahead with a fundamental shift towards networking of forces and capabilities.

The networking paradigm is here today and will only proliferate in the future. Net-centric warfare and net-centric operations are not ends in themselves. Effects Based Operations focus on the mission and the conditions of military operations while NCW provides the framework and tools. They deal with the why, what, how and support of military operations, which are crucial in looking at the military transformation journey.

There is little doubt that the concept of integrated command and control under the context of an IC2 framework can fundamentally change the way we train and fight. It is *real* in that it necessitates the commitment and capacity to change, as transformation is inevitable. This will enable commanders to operate in an ever-changing environment and where the spectrum of operations will require new command and control tools and processes. However, there are major impediments that must be tackled before IC2 can succeed, or else the journey would remain a *myth* to many. These include the need to transform the **culture**, the **structure and processes**, and the ability to sustain support by having **visible deliverables**.

The need to have a shared purpose cannot be ignored since the road to achieving IC2 will be a long one. It must be clear to our operational commanders and warfighters why and what is changing to induce understanding and develop commitment. The switch

to having rigorous debate, discovery and experimentation among warfighters, defense academic and defense scientists will entail a different learning climate.

To be able to fight in an integrated manner and across a spectrum of operations, the net-centric forces must be able to plug quickly into the C2 Information System (CCIS) networks. This will entail interoperable communications, standards, doctrine, tactics and procedures. Joint operating concepts and interoperability must be addressed. The quicker and more complex nature of future operations will require tighter and continuous cooperation among the services. With the new security environment, the need to focus on applicability to other operations like low intensity conflict must be examined. A common operating picture alone will not guarantee that the commanders or staffs viewing it will have the same interpretation (shared understanding / awareness).

While the "fruits" of IC2 may not be realized quickly, dialogue with all levels of commanders should always be maintained to highlight the development and progress (e.g., testing of concepts and results of C2 related experiments). Intermediate products and knowledge gained (whether successful or not) should be shared widely. This will enable commanders and soldiers to be trained and comfortable operating in an information rich environment.

Amidst the excitement of exploring new ways to fight in an integrated environment, core military imperatives will still require that a commander determine the salient points pertinent to his mission and lead his men towards planning and operating successfully in combat. The possibilities offered by embracing NCW and integrated command and control are indeed tremendous. IC2 provides the framework to re-define organizational structures and brings clarity to the orientation of C2 in the information age.

To achieve the next big leap in capability,
IC2 cannot be the dream of just a few
while remaining distant and vague to the rest.

Acronyms

AMSC	Advanced Military Studies Course (Canadian Forces College)
C2	Command and Control
C3	Command, Control and Communications
C4	Command, Control, Communications and Computers
C4I	Command, Control, Communications, Computers and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CCIS	Command and Control Information System
COCOM	Combatant Commander
DoD	Department of Defense (U.S.)
EBO	Effects Based Operations
FCB	Functional Capabilities Board
IC2	Integrated Command and Control
JSAF	Journal of the Singapore Armed Forces
JWID	Joint Warfighter Interoperability Demonstration
NCW	Net-Centric (or Network Centric) Warfare
OODA	Observe, Orient, Decide, Act
OSD	Office of the Secretary of Defense (U.S.)
RMA	Revolution in Military Affairs

References

[Ackerman, 2003] Ackerman, Robert K. "Operation Iraqi Freedom: British Warfighters Exploits Network Centricity", SIGNAL, Sep 2003, 33-37.

[Alberts, 2000] Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP Publication Series, Feb 2000.

[Alberts, 2001] Alberts, David S., et al. Understanding Information Age Warfare. Washington, DC: CCRP Publication Series, Aug 2001.

[Alberts, 2002] Alberts, David S. Information Age Transformation: Getting to a 21st Century Military, CCRP Publication Series, June 2002.

[Alberts, 2003a] Alberts, David S. and Richard E. Hayes. Power to the Edge : Command and Control in the Information Age. Washington, DC: CCRP Publication Series, June 2003

[Alberts, 2003b] Alberts, David S., John J. Garstka, Richard E. Hayes and David A. Signori. Understanding Information Age Warfare. Washington, DC: CCRP Publication Series, Aug 2001.

[APDF, 2002] Asia-Pacific Defense Forum Staff. "JWID 2002: Addressing Coalition Interoperability." Asia-Pacific Defense FORUM, Winter 2002-2003.

[Arndt, 2002] Arndt, Manfred H.H. "Information Age Command and Control – The Weakest Link?" Toronto, Canada: Canadian Forces College Advanced Military Studies Course Paper, 2002.

[Ayling, 2001] Ayling, Brigadier Steve and Sarah Guise. "UNTAC and INTERFET – A Comparative Analysis." Australian Defense Force Journal, No. 150, Sep/Oct 2001, 47-56.

[Blash, 2003] Blash, Edmund C. "Network-Centric Warfare Requires a Closer Look." SIGNAL, May 2003, 56-57.

[Bowley, 2001] Bowley, Dean K. and Steven R. Brewer. "Australia's Regional Environment Blunting the Knowledge Edge?" Australian Defense Force Journal, No. 150, Sep/Oct 2001.

[Boyd, 1986] Boyd, John. "Patterns of Conflict." Unpublished Research. 1986.

[Caterinicchia, 2003] Caterinicchia ,Dan and Mathew French. "Network-centric warfare: Not there yet." Federal Computer Week, June 9 2003, 1-4.

[Cebrowski, 1998] Cebrowski, A. K and J. J. Garstka. "Network Centric Warfare: Its Origin and Future." U.S. Naval Institute Proceedings, Vol. 124, No.1, January 1998, 28-35.

[Chia, 2003] Chia, Aaron E. S. "Countering the Friction and Fog of War in the Information Age." Pointer. Singapore, Malaysia: Singapore Armed Forces: April-June 2003).

[Connor, 2002] Conner, William M. "Emerging Army Doctrine: Command and Control," Military Review, March-April 2002, 80-84.

[Cooper, 1994] Cooper, J. R. Another View of the Revolution in Military Affairs. Carlisle Barracks, PA: U.S. Army War College publication, SSI, 15 Jul 1994, 27.

[Deptula, 2001] Deptula, David A. "Effects-Based Operations: A Change in the Nature of Warfare." Defense and Airpower Series. Arlington VA: Aerospace Education, 2001.

[DoD, 2001] U.S. Department of Defense (DoD). Network Centric Warfare: Department of Defense Report to Congress. Washington DC: U.S. Department of Defense (DoD), 2001.

[Encarta PD] Microsoft Encarta Pocket Dictionary. Redman, WA: Bloomsbury Publishing, Plc., 1999.

[Fargo, 2003] Fargo, Adm. Thomas B. "Strengthening Security in the Asia-Pacific Region." Asia-Pacific Defense Forum, Winter 2002-2003, 2-15.

[FM 100-6, 1996] U.S. Department of the Army. Information Operations. Field Manual 100-6. Washington, DC: Headquarters, U.S. Department of the Army, 27 August 1996.

[FM 6-0, 2003] U.S. Department of the Army. Mission Command: Command and Control of Army Forces. Field Manual 6-0. Washington, DC: Headquarters, U.S. Department of the Army, 11 August 2003.

[Garstka, 2003a] Garstka, John J. "Network-Centric Warfare Offers Warfighting Advantage", SIGNAL, May 2003, 58-60.

[Garstka, 2003b] Garstka, John J. "Network-Centric Warfare: Increased Combat Power for Joint Military Operations." Realizing Integrated Knowledge-based Command and Control, Journal of the SAF, Pointer Monograph No. 2, 2003, 48.

[Hanson, 2001] Hanson, Victor Davis. Carnage and Culture. New York, NY: Doubleday, 2001.

[Jeffery, 2003] Jeffery, Lieutenant-General M. K. Chief of the Land Staff, Canadian Forces. Keynote Address, XXVI Pacific Armies Management Seminar 26-30 August 2003, Calgary, Canada. Script available from http://www2.apan-info.net/pams/pams_xxvi.htm; Internet; accessed 1 October 2003.

[JP1-02, 2003] U.S. Department of Defense. Dictionary of Military and Associated Terms, Joint Publication 1-02. Washington, DC: U.S. Department of Defense, 2003.

[JSAF PM1, 2003] Journal of the Singapore Armed Forces. Creating the Capacity to Change: Defense Entrepreneurship for the 21st Century. Pointer Monograph No. 1, 2003.

[JSAF PM2, 2003] Journal of the Singapore Armed Forces. Realizing Integrated Knowledge-based Command and Control. Pointer Monograph No. 2, 2003.

[Kruzins, 2003] Kruzins, Ed and Jason Scholz. "Australian Perspectives on Network Centric Warfare: Pragmatic Approaches with Limited Resources." Australian Defense Journal, No. 150, Sep/Oct 2003, 19-33.

[Langton, 2002] Langton, Col Christopher. The Military Balance 2002-2003. London, UK: Oxford University Press, 2002.

[Lim, 2003] Lim, LTC Seng Hock. "Myth or Reality: Network Centric Warfare and Integrated Command and Control in the Information Age?" Advanced Military Studies Course Papers #6 (AMSC 6). Toronto, Canada: Canadian Forces College, 2003.

[Mahmud, 2003a] Mahmud, Ghazemy M. "Top Brass Interview: Gen Dato' Wira Mohd Shahrom Bin Dato' HJ Nordin, Chief of Malaysian Army." Asian Defense Journal, 3/2003, 13-18.

[Mahmud, 2003b] Mahmud, Ghazemy M. "Top Brass Interview: Maj Gen Ng Yat Chung, Chief of Defense Force, Singapore." Asian Defense Journal, 7 & 8/2003, 14-18.

[Mak, 1993] Mak, J.N. ASEAN Defense orientation 1975-1992: The Dynamics of Modernization and Structural Change. Canberra, Australia: Strategic and Defense Studies Center, Australia National University, 1993.

[Manfred, 2002] Manfred, A. H. H. "Information Age Command and Control – The Weakest Link?" Advanced Military Studies Course Paper. Toronto, Canada: Canadian Forces College, 2002.

[May, 2001] May, Andrew. "Science forecasting: predicting the unpredictable." Journal of the Defense Science, Vol. 6 No. 2, 2001.

[Mitchell, 2003] Mitchell, Paul T. "Small Navies and Network Centric Warfare," Naval War College Review, Vol. LVI, No. 2, Spring 2003, 83-99.

[O'Hanlon, 2000] O'Hanlon, Michael. Technological Change and the Future of Warfare, Brooking Institution Press, 2000.

[Owens, 2000] Owens, B. Lifting the Fog of War. New York, NY: Farrar, Straus and Giroux, 2000.

[Peter, 1998] Peter, Brook and Thorn Tim. "C3I in the New Defense and Commercial Environments." Journal of Defense Science, Vol. 3, No.1, 1998.

[Pigeau, 2002] Pigeau, Ross & Carol McCann. "Re-conceptualizing Command and Control." Canadian Military Journal, Vol. 3, No. 1, Spring 2002, 53-63.

[Poh, 2003] Poh, Lt. Gen. Lim Chuan. "Realizing Integrated Knowledge-based Command and Control." Journal of the SAF, Pointer Monograph No. 2, *(2003)*.

[Potts, 2002a] Potts, David and Jake Thackray. "No Revolution Please We're British." The Big Issue: Command and Combat in the Information Age, David Potts, ed. London, UK: The Strategic and Combat Studies Institute, March 2002.

[Potts, 2002b] Potts, David. "Tomorrow's War." The Big Issue: Command and Combat in the Information Age, ed. David Potts. London, UK: Strategic and Combat Studies Institute, March 2002.

[Scales, 1998] Scales, Robert H. "Trust, Not Technology, Sustain Coalitions." Parameters, Winter 1998, 4-10.

[Seet, 2003] Seet, Pi S. "The Revolution in Military Affairs: challenge to existing paradigms and its impact on the Singapore Armed Forces (SAF)." Pointer. Singapore, Malaysia: Singapore Armed Forces, April-June 2001, 1-14.

[Sharpe, 2002] Sharpe, G.E. and Allan D. English. Principles for Change in the Post-Cold War Command and Control of the Canadian Forces. Kingston, ON: Canadian Forces Leadership Institute, 2002.

[Sherman, 2003] Sherman, Jason. "Requirement Revolution." Defense News, 4 August 2003, 1.

[Smith, 2002] Smith, Edward A. Effects Based Operations: Applying Network Centric Warfare in Peae, Crisis, and War. Washington, DC: CCRP Publication Series, Nov 2002.

[Snider, 2003] Snider, Don M. "Jointness, Defense Transformation, and the Need for a New Joint Warfare Profession." Parameters, Autumn 2003, 17-30.

[Thackray, 2002] Thackray, Jake. "The Holy Grail." The Big Issue: Command and Combat in the Information Age. David Potts, ed. London, UK: Strategic and Combat Studies Institute, March 2002, 26.

[Thomas, 2000] Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." Parameters, U.S. War College Quarterly, Spring 2000, 13-29.

[Tzu, 1985] Tzu, Sun. The Art of War. Translated by Lionel Giles. London, UK: Stackpole Brooks, 1985.

[Van Creveld, 1985] Van Creveld, Martin. Command in War. Cambridge, MA: Harvard University Press, 1985.

[Watanabe, 1995] Watanabe, Frank. "Understanding the RMA." Armed Forces Journal International, August 1995, 6.

[Young, 2003] Young, Thomas D. "The Revolution in Military Affairs and Coalition Operations: Potential Problem Areas and Solutions." NPGS RMA Paper. Monterey, CA: Naval Postgraduate School (NPGS), 24 Jul 2003.

[Zainal, 2003] Zainal, Maj. Gen. Dato' Abdul Aziz. "Achieving Interoperability Across a Capability Gap between Partners." Presented at the XXVI Pacific Armies Management Seminar, 26-30 August 2003. Calgary, Canada: 2003.

End Notes

[1] [Van Creveld, 1985]

[2] The observation made in 1965 by Gordon Moore, co-founder of Intel, that the number of transistors per square inch on integrated circuits had doubled every year since the integrated circuit was invented. Moore predicted that this trend would continue for the foreseeable future. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every 18 months, and this is the current definition of Moore's Law, which Moore himself has blessed. Most experts, including Moore himself, expect Moore's Law to hold for at least another two decades

[3] Metcafe's Law is an assertion by Robert Metcalfe, founder of 3Com Corporation and designer of the Ethernet protocol for computer networks. It states that "the usefulness, or utility, of a network equals the square of the number of users." For example, the Internet reached critical mass in 1993, when there were roughly 2.5 million host computers on the network, and by November 1997, the Internet contained approximately 25 million host computers.

[4] As highlighted by the Gilder's Law, an assertion by George Gilder, visionary author of Telecosm, which states that "bandwidth grows at least three times faster than computer power." This means that if computer power doubles every eighteen months (per Moore's Law), then communications power doubles every six months.

[5] This operations refers to the military objective by allied forces to degrade and damage the military and security structure that Yugoslav President Milosevic has used to depopulate and destroy the Albanian majority in Kosovo. (From a prepared statement of William S. Cohen, Secretary of Defense, to the Senate Armed Services Committee on 15 April 1999.)

[6] This is the first sentence of the Executive Summary of the Network Centric Warfare Department of Defense Report to Congress in July 2001 according to Alberts and Hayes [Alberts, 2003a].

[7] An example was illustrated in [Cebrowski, 1998] on how Wal-Mart achieved the competitive advantage by having a sensory grid of point-of-sale scanners which collect information and share them with the suppliers in near real time.

[8] Blash [Blash, 2003] contended that NCW is optimized for a lighter logistical "tail" component, hence it may not be suitable for all forms of warfare.

[9] Australia wanted a pragmatic approach and sees this as being a mechanism for seeking a Joint capability focus. For details refer to [Kruzins, 2003].

[10] In [Alberts, 2002] - they were referring to the definition in [JP1-02, 2003].

[11] This definition was shown in their presentation to the Canadian Forces College on 18 September 2003 entitled: "A New Conceptual Framework for Command and Control."

[12] Boyd, John R. Patterns of Conflict: A Discourse on Winning and Losing. Unpublished Research. http://www.defense-and-society.org/FCS_Folder/boyd.htm#discourse. Boyd's monumental look at what makes any organization competitive. Encompassing 2,500 years of the history of conflict, this briefing introduces his famous "OODA loop" concept. The OODA Loop was created by LtCol Boyd's observations on his own decision/action cycle as a USAF jet pilot fighting MIG-15s in the Korean War.

[13] C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) encompasses the entire sensors spectrum and how they are linked to provide intelligence and awareness.

[14] Adapted from David S Alberts, et al, *Understanding Information Age Warfare*, CCRP Publication Series, Aug 2001, 146) [Alberts, 2001].

[15] Presented by Major General Dato' Abdul Aziz Zainal at the XXVI Pacific Armies Management Seminar, 26 – 30 August 2003 at Calgary, Canada, entitled "Achieving Interoperability Across a Capability Gap between Partners." Presentation script available from http://www2.apan-info.net/pams/pams_xxvi.htm.

[16] Highlighted by the ex-CDF of SAF, Lt. Gen. Lim Chuan Poh, in [Poh, 2003].

[17] Adapted from Ravinder Singh, et al, "IKC2 for the SAF – Organizing around Knowledge", in *Realizing Integrated Command and Control,* Journal of the SAF, Pointer Monograph No. 2,2003, 14. [JSAF PM2, 2003]

Implementing Network-Centric Command And Control

10th International Command and Control Research and Technology Symposium
The Future of C2

Raymond J. Curts, Ph.D., (CDR, USN Ret.)
CommIT Enterprises, Inc.
Arlington, Virginia
raymond.curts@commitent.com
(703) 731-0301

Joseph P. Frizzell, PhD
ASD(NII) C2 Policy Directorate
Crystal Mall 3, Suite 6000
1851 South Bell Street
Arlington, VA 22202
(703) 607-0713
joseph.frizzell@osd.mil

Agenda

- The Goal
- Background
- Premise
- The Network-Centric Report
- Sharing
- Trust
- Key Ingredients Of IC2
- Conclusion

The Goal

"By making possible a faster, clearer reading of the situation and a more effective distribution of resources, a superior command system may serve as a force multiplier and compensate for weaknesses in other fields…"

- Martin van Creveld, 1985

Background

- The field of Command, Control, Communications and Computers (C4) is moving so quickly that the interaction between user pull and technology push is becoming exceptionally dynamic.
- Advancements in C4, sensors, information, information systems and precision-strike technologies, as well as the implementation of new, broad, ubiquitous networks, are creating a significant change in the military information environment.

Our Premise

- It will be some time before U.S. military forces can achieve a truly interoperable command and control capability because significant impediments relating to:
  - ***culture,***
  - ***structures,***
  - ***processes, and***
  - ***products***

  must first be addressed.

Network Centric Warfare Report

- As described in the Network Centric Warfare Report to Congress, a fighting force that can conduct network centric operations can be described as having the following attributes and capabilities:
  - **Physical Domain**: All elements of the force are robustly networked achieving secure and seamless connectivity.
  - **Information Domain**: The force has the capability to collect, share, access and protect information. The force can collaborate in the information domain.
  - **Cognitive Domain**: The force has the capability to develop and share high quality situational awareness and have a shared knowledge of the commanders' intent.

Sharing

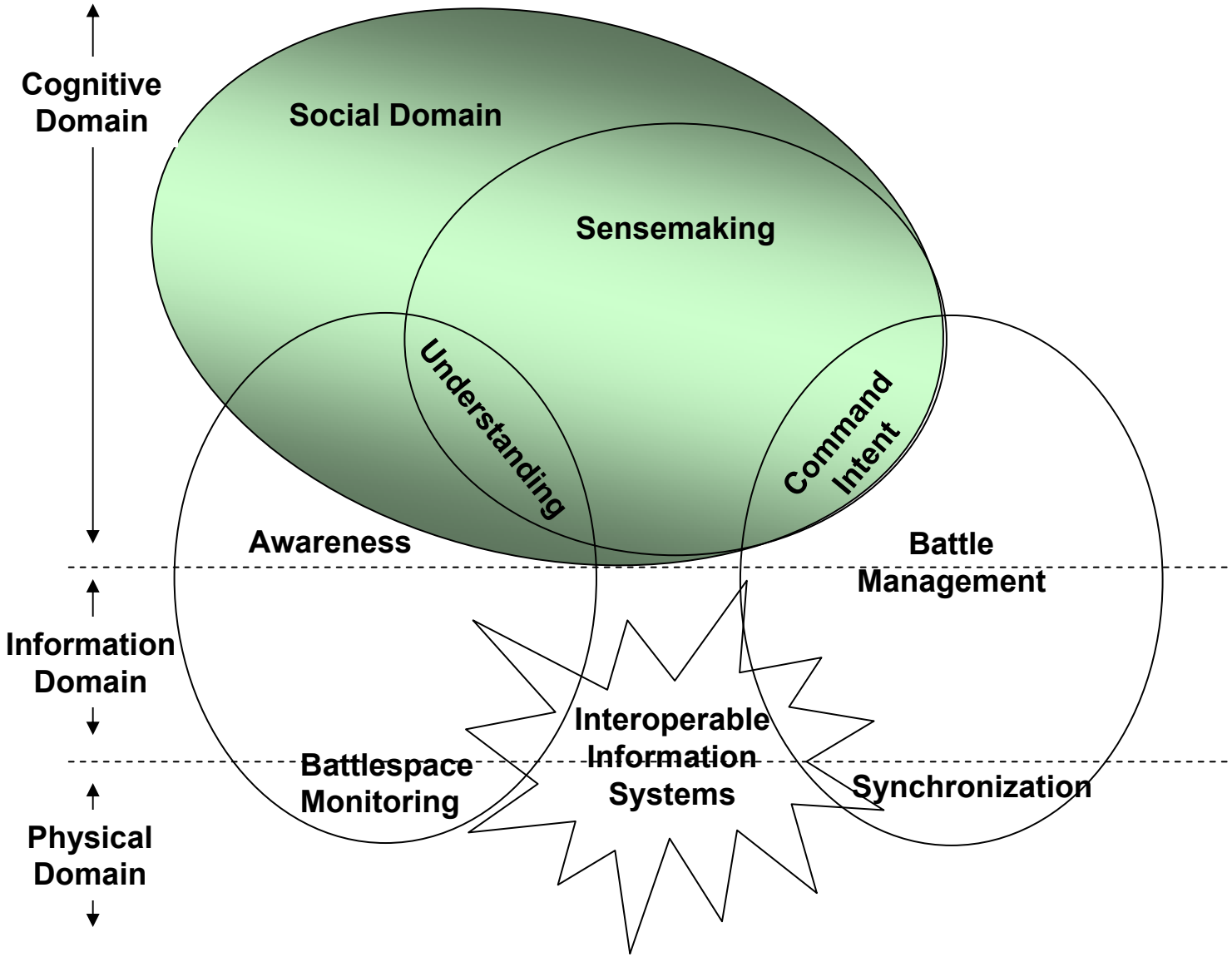
- All of these domains require a ***shared*** networking environment, ***shared*** information and knowledge, ***shared*** situation awareness and understanding of commander's intent. By definition, ***shared*** implies:
  - The use of something along with others.
  - Letting someone use something.
  - Having similar feeling or experience.
  - Taking responsibility together.

I.e., Sharing is a Social concept!

The Social Domain

- Besides the physical, information and cognitive, domains the **social domain** (the domain of sharing & interaction) is also needed.
- **Social Domain**: The social domain implies the **cultural** impact that can create the kind of understanding that will promote *shared* interaction and proceedings congruent to the commander's intent.
- C2 processes and the interactions between and among individuals and entities that fundamentally define organization and doctrine exist in the social domain.

Information Age C2 Process



Interoperability

- To have an effective and robustly networked force, there is a need to have an enterprise-wide, integrated C2 system.
- Such a force can only be achieved if there is high interoperability among mission participants, data elements and the systems that support them.
  - Interoperability ensures the ability of systems and forces to interact effectively with other systems and forces.
  - Forces that are interoperable are able to operate in a net-centric environment.

Shared Awareness

- Interoperability in the social domain allows actions to be dynamically self-synchronized (the ability for commanders to support one another without detailed prior coordination due to shared awareness, in other words, ***trust***).

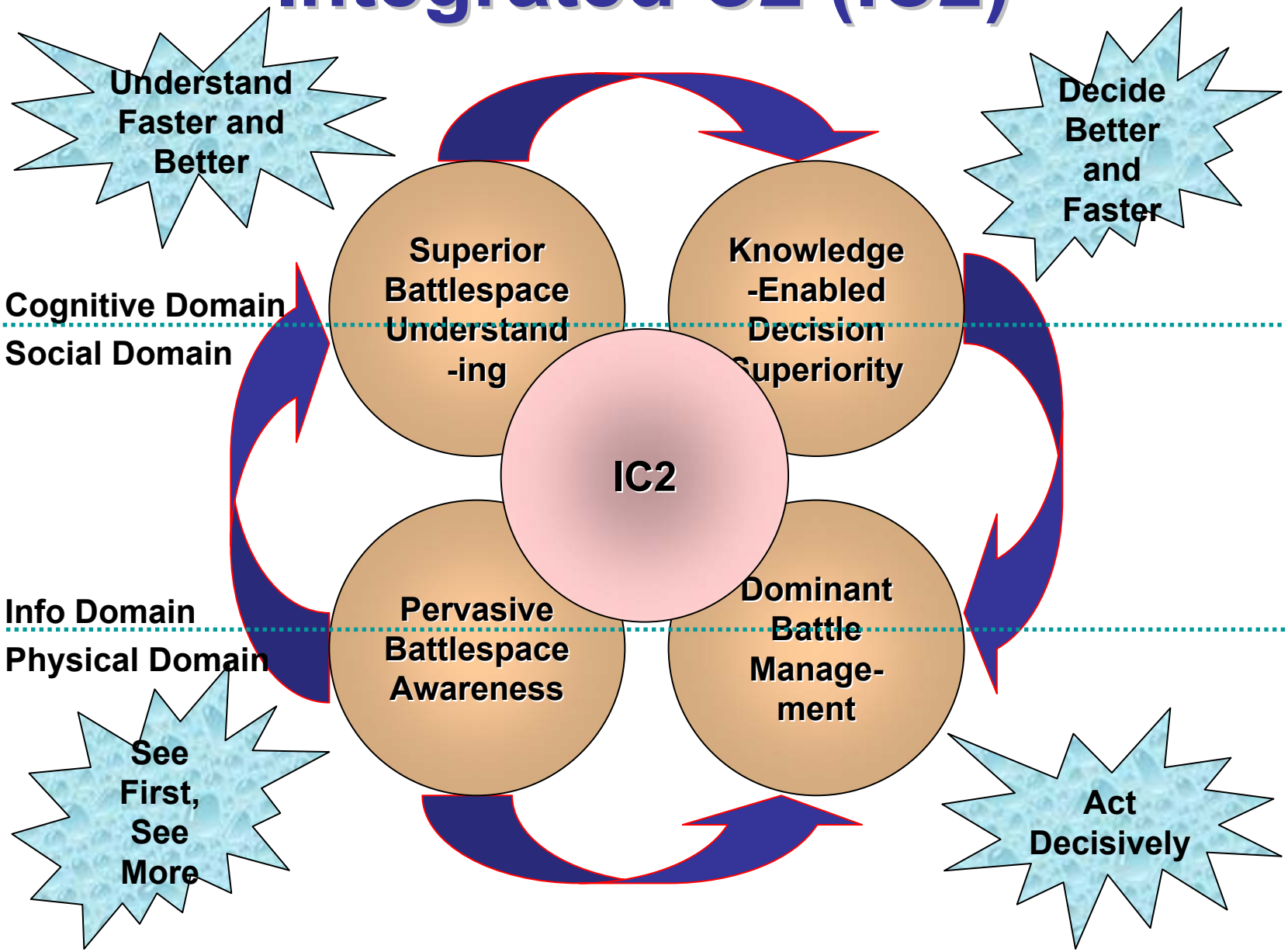
- The social domain implies the **cultural** impact that can create the kind of understanding that will promote interaction and actions congruent to the commander's intent.

Integrated C2 (IC2)

- Command and control is as much about the technology and the **processes** that enable it, as it is about the commanders and their staffs who use the technology and processes.

- ***Integrated*** refers to the need to fight as an synchronized, harmonized, multi-dimensional force.

Integrated C2 (IC2)



Key Ingredients

- The following are considered key to achieving IC2:
  - ***Culture***
  - ***People***
  - ***Trust***
  - ***Time***
  - ***Structure***
  - ***Process***
  - ***Products***
  - ***Organization***

Culture

- The *capacity to change* is as much about looking at fundamentally different strategic "options" as it is changing the *mindsets of people* to "dare" to look at radical changes and to experiment.
- The **military *culture*** is an important consideration if evolutionary, and in some cases revolutionary, operational concepts are to be tested objectively and evaluated fairly.

People

- Culture, by definition, is "… ***people*** with shared beliefs and practices …."
- The importance of people is often cited in reports of change and to really enable transformation and harness the power of IC2, the need for a common purpose cannot be ignored if we intend to accelerate the change.

Trust

- ***Trust*** is believing. It alleviates having to confirm or verify, and eliminates the requirement to know first hand that something has been successfully accomplished.
- ***Trust*** is a learned quality derived from faith in the system and those who are part of it, and is based on mutual understanding, commitment, conviction and dedication.

Time

- The excitement surrounding a technologically enabled transformation could quickly fade if progress is not ***time***ly.
- Policy must clearly define roles and responsibilities, and commanders must set priorities such that work objectives are defined at manageable levels to fit within existing time constraints.

Structure

- Sun Tzu observed that *"… just as water retains no constant shape, so in warfare there are no constant conditions …."* emphasizing the need to have continuous adaptation and superior battlespace awareness and understanding.
- This fluidity, however, strains C2 ***structures*** & resources and significantly increases the complexity of policy development.

Process

- Well defined and tested ***processes*** are necessary to support the structure and the full spectrum of joint operations envisioned by the Goldwater Nichols legislation.
- Joint forces, able to “plug” quickly into an integrated battlespace structured around interoperable communications, standards, doctrine, tactics and procedures, benefit from greater adaptability and a superior sense of battlespace awareness.

Products / Deliverables

- **Visible *deliverables*** become important, both politically and operationally, to sustain the transformation journey towards IC2.
- ***Products*** that are based on an integrated C2 architecture will give the services a quantum leap in capabilities when combined with battlespace awareness and precision strike.

Organization

- Within DoD there are currently multiple ***organizations*** with varying levels of responsibility for C2 functions, processes, procedures, policies and operational concepts. In addition, each of these organizations sponsors a number of C2 or C2-related initiatives and there does not seem to be any central coordination that will ultimately ensure an enterprise-wide IC2 environment.

Even if these were all perfectly coordinated, the construct is

extremely difficult to work within.

Authority / Responsibility

- Some entity must accept the ***responsibility for*** and be empowered with the ***authority to***:
  - integrate / coordinate C2 architectures and programs across DoD,
  - assist with the development of and endorse C2 policies and directives,
  - represent the C2 community at large within the Integrated C2 enterprise-wide governance structure.

Governance

- There must be ***governance*** to support and enforce the development a *culture* of *trust* within and among *people* and *organizations*, to adhere to *time*-frames and to develop the *structures*, *processes* and *products*, that will deliver the full range of Integrated C2.
- ***Policy, guidance*** and ***governance*** are the glue that will help to coordinate and hold the key components together.

Conclusion

To achieve the next big leap in capability,

IC2 cannot be the dream of just a few

while remaining distant and vague to the rest.

Implementing Network-Centric Command And Control

10th International Command and Control Research and Technology Symposium
The Future of C2

Raymond J. Curts, Ph.D., (CDR, USN Ret.)
CommIT Enterprises, Inc.
Arlington, Virginia
raymond.curts@commitent.com
(703) 731-0301

Joseph P. Frizzell, PhD
ASD(NII) C2 Policy Directorate
Crystal Mall 3, Suite 6000
1851 South Bell Street
Arlington, VA 22202
(703) 607-0713
joseph.frizzell@osd.mil